ARC 4965C

SECRETARY OF STATE[721]

Notice of Intended Action

Proposing rule making related to elections technology security and providing an opportunity for public comment

The Secretary of State hereby proposes to amend Chapter 29, "Elections Technology Security," Iowa Administrative Code.

Legal Authority for Rule Making

This rule making is proposed under the authority provided in Iowa Code section 47.1.

State or Federal Law Implemented

This rule making implements, in whole or in part, Iowa Code section 47.1.

Purpose and Summary

While the Secretary of State's office has seen tremendous voluntary adoption of services and security best practices, there is more work to do to continue to increase the security of Iowa's elections. The amendments proposed in this rule making will bolster election security by requiring county commissioners of elections to uniformly adopt best practices.

Fiscal Impact

This rule making has no fiscal impact to the State of Iowa.

Jobs Impact

After analysis and review of this rule making, no impact on jobs has been found.

Waivers

Any person who believes that the application of the discretionary provisions of this rule making would result in hardship or injustice to that person may petition the Secretary of State for a waiver of the discretionary provisions, if any, pursuant to 721—Chapter 10.

Public Comment

Any interested person may submit written comments concerning this proposed rule making. Written comments in response to this rule making must be received by the Secretary of State no later than 4:30 p.m. on March 31, 2020. Comments should be directed to:

Eric Gookin
Office of the Secretary of State
Lucas State Office Building
321 East 12th Street
Des Moines, Iowa 50319
Email: eric.gookin@sos.iowa.gov

Public Hearing

No public hearing is scheduled at this time. As provided in Iowa Code section 17A.4(1)"b," an oral presentation regarding this rule making may be demanded by 25 interested persons, a governmental

subdivision, the Administrative Rules Review Committee, an agency, or an association having 25 or more members.

Review by Administrative Rules Review Committee

The Administrative Rules Review Committee, a bipartisan legislative committee which oversees rule making by executive branch agencies, may, on its own motion or on written request by any individual or group, review this rule making at its regular monthly meeting or at a special meeting. The Committee's meetings are open to the public, and interested persons may be heard as provided in Iowa Code section 17A.8(6).

The following rule-making actions are proposed:

ITEM 1. Amend subrule 29.3(1) as follows:

29.3(1) A commissioner who identifies or suspects an actual or possible cybersecurity incident or breach shall immediately report the incident to the state commissioner. Upon receiving the report, the state commissioner shall alert the appropriate state or federal law enforcement agencies, including but not limited to the ~~federal~~ United States Department of Homeland ~~Security,~~ Security's Cybersecurity and Infrastructure Security Agency (CISA) and the OCIO, and the vendor responsible for maintaining the affected technology. The state commissioner may disseminate the information to other federal, state, and local agencies, or their designees, as the state commissioner deems necessary.

ITEM 2. Adopt the following **new** rule 721—29.4(47):

721—29.4(47) Election security by the commissioners.

29.4(1) At the start of each year, the commissioner shall provide to the state commissioner the following information:

a. The full personnel roster and email addresses of the commissioner's office that identifies who from the office will participate in election administration in any form throughout the year. This does not include precinct election workers.

(1) The roster will identify the personnel that the commissioner considers critical to the successful execution of elections.

(2) The roster will further identify a technical point-of-contact (POC) for the state commissioner. If the commissioner wishes to serve as the POC, the commissioner will also designate an additional POC. The POC needs to be a government employee but does not necessarily need to be a person within the commissioner's office.

b. A list of other county employees who may be involved in the event of an incident in the county.

29.4(2) Every commissioner shall be a member of the Elections Infrastructure Information Sharing and Analysis Center. The state commissioner shall provide information on how to become a member upon request by a commissioner.

29.4(3) In every odd-numbered year, every commissioner shall request the following services from CISA. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than CISA for substantively similar services. A failure of CISA to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

a. Cyber resilience review.

b. Risk and vulnerability assessment.

c. External dependencies management assessment.

d. Remote penetration testing.

e. Protective security assessment.

29.4(4) Every commissioner shall utilize the following services from OCIO. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than OCIO

for substantively similar services. A failure of OCIO to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

a. Intrusion detection system.

b. Host and network malware detection.

c. Cybersecurity training, including phishing assessments.

d. Vulnerability management.

29.4(5) Every commissioner shall request a weekly vulnerability scanning by CISA.

29.4(6) A commissioner shall remediate all critical or high-risk vulnerabilities identified by any assessment.

29.4(7) The state commissioner may require every commissioner and commissioner's staff to participate in phishing assessments.

29.4(8) Commissioners may choose to participate in any other assessments or testing from vendors approved by the state commissioner. Commissioners shall notify the state commissioner when any assessments are scheduled.

29.4(9) The state commissioner may require a commissioner and commissioner's staff to participate in any assessment or training that the state commissioner arranges.

29.4(10) No commissioner shall permit the use of personal email for the conduct of elections. This applies to all full-time and part-time staff of the commissioner as well as the commissioner. No other full-time and part-time employees of the county who assist in any part of the administration or security of elections are permitted to use personal email for the conduct of elections. However, this does not apply to precinct election officials who are not normally employed by the county on a regular basis in another capacity. This prohibition applies to forwarding election business emails to a personal email address. This does not include out-of-band emails created as a part of a continuity of government plan or an incident response plan.

29.4(11) Any county information technology infrastructure that is used to access or conduct any part of elections in the state is subject to the following requirements:

a. Passwords to access the county network must be compliant with the standards enumerated by either the National Institute of Standards and Technology or guidance issued by the state commissioner.

b. Network timeout standards must be compliant with the standards enumerated by either the National Institute of Standards and Technology or guidance issued by the state commissioner.

c. A current inventory of IT assets assigned to the commissioner's office shall be kept.

d. Periodic back-ups of data belonging to assets within the commissioner's office shall be made.

29.4(12) The website of a commissioner shall have a top-level domain of ".gov" and shall utilize secure socket layer or transport layer security certificates for all publicly facing websites. A commissioner's agreement with OCIO to use a subdomain of ".iowa.gov" is sufficient to satisfy this requirement. A commissioner's site that redirects traffic from a different top-level domain to a ".gov" domain is sufficient to satisfy this requirement.

29.4(13) If the state commissioner is satisfied that a county has an adequate alternative to any requirement in this rule, the state commissioner may waive that requirement. It is the sole discretion of the state commissioner whether a county qualifies for a waiver.

29.4(14) Except where otherwise exempted, failure by a commissioner to follow these rules constitutes a technical violation pursuant to Iowa Code section 39A.6.

ITEM 3. Adopt the following **new** rule 721—29.5(47):

721—29.5(47) Emergency or incident response plans.

29.5(1) Every commissioner shall have an election security incident response plan. A commissioner whose election-specific plan is part of a larger county-level emergency response plan, continuity of government plan, or incident response plan satisfies this requirement.

29.5(2) Every commissioner shall review the plan at least annually and make updates as necessary.

29.5(3) A commissioner shall provide the plan to the state commissioner at the state commissioner's request.

29.5(4) Information shared under this rule shall retain protection as a nonpublic, confidential record pursuant to Iowa Code section 47.1(6).

ITEM 4. Adopt the following **new** rule 721—29.6(47):

721—29.6(47) Social media accounts.

29.6(1) A commissioner using a social media account for official county business shall request "verified" or similar recognition. The state commissioner shall provide information on the subject upon request by a commissioner.

29.6(2) A commissioner using a social media account shall protect the account using multifactor authentication.

29.6(3) The state commissioner may require that commissioners use additional security measures for social media accounts, based on emerging best practices.